DERWENT-ACC-NO: 2000-272587

DERWENT-WEEK: 200149

TITLE: Data **encryption** standard coding protection method - **varying order** of evaluation of substitution boxes using random number generator

INVENTOR: SEDLAK, H; VELTEN, J

PATENT-ASSIGNEE: SIEMENS AG[SIEI] , INFINEON TECHNOLOGIES AG[INFN]

PRIORITY-DATA: 1998DE-1045073 (September 30, 1998)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
DE 19845073 A1	April 6, 2000	N/A	004	G06F 012/14
DE 19845073 C2	August 30, 2001	N/A	000	G06F 012/14

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
DE 19845073A1	N/A	1998DE-1045073	September 30, 1998
DE 19845073C2	N/A	1998DE-1045073	September 30, 1998

INT-CL (IPC): G06F012/14, G06K019/073 , H04L009/06

ABSTRACTED-PUB-NO: DE 19845073A

BASIC-ABSTRACT:

The protection method involves **preventing the encryption** key from being extracted by differential power **analysis of the encryption** processor by **varying the order** for the evaluation of the substitution boxes, e.g. under control of a random-number generator. The

evaluation for some or all of the substitution boxes may be doubled, with the sequence of the double evaluation also varied and random wait states inserted between the individual substitution box evaluations.

USE - For protecting sensitive data.

ADVANTAGE - **Prevents** extraction of encryption key by power **analysis**.

CHOSEN-DRAWING: Dwg.1/2

TITLE-TERMS: DATA **ENCRYPTION** STANDARD CODE PROTECT METHOD **VARY ORDER** EVALUATE SUBSTITUTE BOX RANDOM NUMBER GENERATOR

DERWENT-CLASS: T01 T04 T05 W01

EPI-CODES: T01-D01; T01-H01C2; T04-K; T05-L02; W01-A05A;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N2000-204209

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 45 073 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
G 06 K 19/073
H 04 L 9/06

(21) Aktenzeichen: 198 45 073.7
(22) Anmeldetag: 30. 9. 1998
(43) Offenlegungstag: 6. 4. 2000

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Velten, Joachim, 35216 Biedenkopf, DE; Sedlak, Holger, 85658 Egmating, DE

(56) Entgegenhaltungen:
US 57 96 837

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Absicherung der DES-Verschlüsselung gegen Ausspähung der Schlüssel durch Analyse der Stromaufnahme des Prozessors

(57) Verfahren zur Absicherung der DES-Verschlüsselung gegen Ausspähung der Schlüssel durch Analyse der Stromaufnahme des Prozessors, wobei die Reihenfolge der Auswertung der S-Boxen in jeder DES-Runde zufallsabhängig verändert wird. Zusätzlich können einige oder alle S-Boxen doppelt ausgewertet werden.

DE 198 45 073 A 1

DE 198 45 073 A 1

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zur Absicherung der DES-Verschlüsselung gegen Ausspähung der Schlüssel durch Analyse der Stromaufnahme des Prozessors.

Das DES-Verfahren (DES = Data Encryption Standard) wurde bereits in der Mitte der 70er Jahre entwickelt und ist heute weit verbreitet zur Absicherung von Daten, beispielsweise bei der elektronischen Überweisung von Geldbeträgen. Der DES-Standard ist als ANSI X3.92 standardisiert.

Das DES-Verfahren funktioniert folgendermaßen:
Die zu verschlüsselnden Daten werden in Blöcke von 64 Bit zerlegt. Jeder Block wird separat verschlüsselt, indem ein ebenfalls aus 64 Bit bestehender Schlüssel verwendet wird. Dazu wird der Block gemäß einer vorgegebenen Verfahrensweise permutiert, und dann in eine linke und eine rechte Hälfte geteilt. Es erfolgen dann 16 Durchgänge einer identischen Operation (genannt Funktion F) in der die Daten mit dem Schlüssel kombiniert werden. Nach der 16. Runde werden die Daten wieder zu einem einzelnen 64-Bit-Block zusammengesetzt und dann ein letztes Mal permutiert, wobei diese zweite Permutation die inverse Operation zu der ersten darstellt.

In den einzelnen Runden wird jedes 8. Bit des DES-Schlüssels ignoriert, so daß die verbleibenden 56 Bit zur Verschlüsselung herangezogen werden. Dabei werden diese 56 Bit in jeder der 16 Runden abhängig von der Runde um ein oder zwei Bit nach links verschoben. Daraus werden dann jeweils 48 Bit für die Funktion F ausgewählt. Zuerst werden dann die rechten 32 Bit durch eine Expansionspermutation auf 48 Bit expandiert, sodann mit den 48 ausgewählten Bits des Schlüssels durch eine Ausschließlich-Oder-Operation (XOR) verknüpft. Diese 48 neuen Bit werden in 6-Bit-Gruppen zerlegt und durch 8 "Substitution-Boxes" oder S-Boxen geschickt, die aus den 6-Bit 4-Bit-Gruppen erzeugen. Der Abschluß der Funktion F ist die Permutation der 32 so erhaltenen Bits. Der Ausgangswert der Funktion F wird dann mit der linken Hälfte der 64 Bit durch eine weitere XOR-Operation verknüpft. Das Ergebnis dieser Operation wird die neue rechte Hälfte und die alte rechte Hälfte wird die neue linke Hälfte.

Der Vorteil von DES liegt darin, daß die Entschlüsselung mit genau dem selben Verfahren erfolgen kann, und lediglich die 48-Bit-Schlüssel jeder Runde in umgekehrter Reihenfolge wie bei der Verschlüsselung verwendet werden müssen.

Zur Zeit seiner Entwicklung hielt man dieses Verschlüsselungsverfahren für praktisch nicht zu knacken, da damals solche Verschlüsselungsverfahren nur auf Großrechnern ablaufen konnten. Heutzutage stellt sich aber das Problem, daß auch intelligente Chipkarten, d. h. Chipkarten mit Prozessor, solche Verschlüsselungsverfahren verwenden sollen. Bei einer Chipkarte besteht jedoch die Möglichkeit, jeweils den zeitlichen Verlauf der Stromaufnahme der Karte, der im wesentlichen der Stromaufnahme des auf der Karte montierten Prozessors entspricht, zu messen, während die Karte eine Verschlüsselungsoperation durchführt.

Hierbei kann nun einfach die Stromaufnahme während des Arbeitens des Prozessors auf der Karte gemessen werden. Dies nennt sich "Simple Power Analysis (SPA)". Es ist jedoch relativ einfach, Chipkarten zu bauen, die gegen die Simple Power Analysis widerstandsfähig sind.

Es ist jedoch auch möglich, nicht einen Verschlüsselungsvorgang wie bei der SPA zu beobachten, sondern eine Serie von Verschlüsselungsvorgängen mit dem gleichen Schlüssel. Es lassen sich dann durch Überlagerung der einzelnen zeitlichen Abläufe der Stromaufnahme und durch statistische Auswertung dieser Messungen, Rückschlüsse über den verwendeten Schlüssel ziehen.

Es ist daher Aufgabe der vorliegenden Erfindung, eine Ermittlung der Schlüssel auch bei Beobachtung der Stromaufnahme des Prozessors und auch unter Verwendung von "Differential Power Analysis" erheblich zu erschweren oder ganz zu verhindern.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, daß die Reihenfolge der Auswertung der S-Boxen verändert wird.

Besonders bevorzugt ist es dabei, die Reihenfolge der Auswertung der S-Boxen in jeder DES-Runde zu verändern.

Dabei ist es besonders günstig, die Reihenfolge der Auswertung der S-Boxen jeweils durch einen Zufallsgenerator zu steuern.

Eine weitere Absicherung gegen statistische Analysen kann dadurch erfolgen, daß zusätzlich einige oder alle S-Boxen doppelt ausgewertet werden, wobei auch hier die Reihenfolge der doppelten Auswertungen nochmals verändert werden kann.

Eine noch weiter gehende Entkopplung zwischen der Stromaufnahme des Prozessors und den verwendeten Schlüsseln kann dadurch erzielt werden, daß zusätzlich noch zufällig verteilte Prozessorwartezyklen zwischen die einzelnen S-Box-Auswertungen eingeschoben werden.

Im folgenden wird die Erfindung anhand eines Ausführungsbeispiels näher erläutert. Es zeigen:

Fig. 1 den Verlauf der Stromaufnahme bei einem Programmablauf gem. dem Stand der Technik; und

Fig. 2 den Verlauf der Stromaufnahme bei der erfindungsgemäßen Lösung.

Die bekannten DES (Data Encryption Standard) Softwarerealisierungen auf Chipkarten (ICC) lassen sich mittels der "Differential Power Analysis" (DPA) angreifen.

DPA nutzt jede Daten bzw. Adressabhängigkeit der ICC-Stromaufnahme aus. Bestimmte Operationen lassen sich in der ICC bzw. deren Microcode derart optimieren, daß keine Datenabhängigkeit in der Stromaufnahme zu erkennen ist. Dies ist z. B. bei der Klasse der Bitbefehle gelungen, d. h. nach der Portierung eines Standard DES-Programms auf eine derartige TCC ist nur noch ein DPA-Peak in den Stromprofilen nachweisbar. Dieser Peak wird von der S-Box Auswertung in der 15. Runde des DES-Algorithmus hervorgerufen (gleiches gilt jedoch auch für den Angriff auf die ersten DES Runden).

Hierbei wird aus jeweils 6 Bit der Expansionsabbildung E ein 4 Bit Ergebnis abgeleitet, welches nach entsprechender Weiterverarbeitung als Eingangsdatum für die letzte DES Runde dient.

Diese Auswertung wird üblicherweise mittels im ROM bzw. EEPROM abgelegten Tabellen durchgeführt. Die Erkennbarkeit im Stromprofil rührt daher, daß je nach dem, auf welches Tabellenelement zugegriffen werden soll, entsprechende, stromintensive Änderungen auf dem Adressbus der CPU vorgenommen werden müssen. Derzeit sind gegen diesen Effekt keine einsetzbaren Hardwaremaßnahmen bekannt.

Die gute Erkennbarkeit dieses in **Fig.** 1 dargestellten DPA-Peaks rührt daher, daß die Auswertung der S-Boxen immer in dem selben zeitlichen Raster und der selben Reihenfolge vorgenommen wird.

Zur Verschleierung dieses DPA-Peaks wird erfindungsgemäß das folgende Verfahren vorgeschlagen:
Die Reihenfolge der Auswertung der S-Boxen wird durch einen Zufallsgenerator gesteuert. Das heißt, die ursprüngliche Auswertungsreihenfolge s1, s2, s3, s4, s5, s6, s7, s8 wird z. B. bei einer DES-Runde in die Folge s2, s3, s1, s6, s7, s5, s4, s8 umgesetzt. Bei der nächsten DES-Runde wird z. B.

die Auswertung in der Reihenfolge s1, s6, s4, s8, s2, s3, s7, s5 vorgenommen. Zusätzlich kann ggf. eine doppelte Auswertung von S-Boxen vorgenommen werden, z. B. also s1, s6, s4, s8, s2, s3, s7, s1, s4, s5. Hierdurch kann eine zusätzliche zeitliche Verjitterung der DES-Ausführung erreicht werden.

Da bei der DPA eine große Anzahl von Messungen benötigt wird, erhält man erfindungsgemäß das in **Fig.** 2 dargestellte Stromprofil (wobei die Fläche unter den Peaks in beiden Fällen wegen der Statistik wohl gleich ist).

Durch diese Maßnahme wird ein großer Peak in mehrere kleine Peaks aufgeteilt. Hierdurch wird der Aufwand für den Angreifer höher:

- mehr Messungen sind notwendig, um eine eindeutige Erkennbarkeit zu gewährleisten, wegen des nun schlechteren Signal/Rauschverhältnisses;
- durch das Einschalten des Random Wait State Generators wird der Aufwand für den Angreifer nochmals gesteigert.

Die Darstellung dieser kleinen Peaks in **Fig.** 2 ist nämlich nur möglich, wenn

- die erfindungsgemäß randomisierte S-Box Auswertung immer im selben Zeitraster vorgenommen wird und
- der Angreifer geeignete Verfahren hat, um die erste S-Box Auswertung als Startpunkt für seine Auswertung zu erkennen.

Diese Punkte lassen sich durch geeignete Software- und Hardwaremaßnahmen weiter erschweren:

- zeitliche Verjitterung der DES-Ausführung
- Random Wait State Generator
- Current Scrambling Engine.

Patentansprüche

1. Verfahren zur Absicherung der DES-Verschlüsselung gegen Ausspähung der Schlüssel durch Analyse der Stromaufnahme des Prozessors, **dadurch gekennzeichnet**, daß die Reihenfolge der Auswertung der S-Boxen verändert wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Reihenfolge der Auswertung der S-Boxen in jeder DES-Runde verändert wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Reihenfolge der Auswertung der S-Boxen jeweils durch einen Zufallsgenerator gesteuert wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß zusätzlich einige oder alle S-Boxen doppelt ausgewertet werden, wobei auch hier die Reihenfolge der doppelten Auswertungen nochmals verändert werden kann.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß zusätzlich noch zufällig verteilte Prozessorwartezyklen (random wait states) zwischen die einzelnen S-Box-Auswertungen eingeschoben werden.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 198 45 073 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 6. April 2000

FIG 1

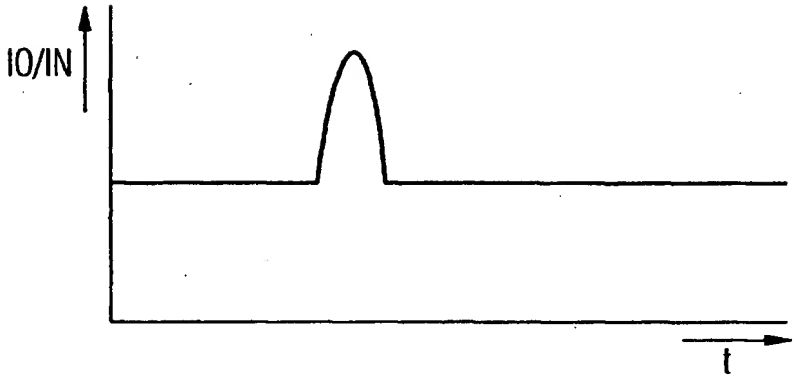
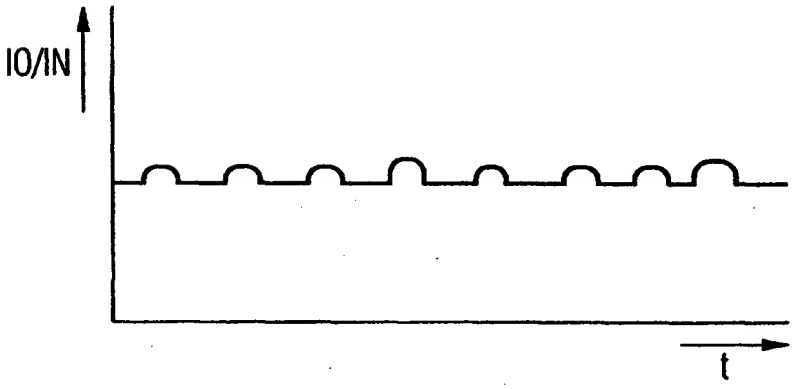


FIG 2



IDS REFERENCES

☐ FOR